Bank of Canada Banque du Canada

Working Paper 2003-2 / Document de travail 2003-2

Managing Operational Risk in Payment, Clearing, and Settlement Systems

by

Kim McPhail

ISSN 1192-5434

Printed in Canada on recycled paper

Bank of Canada Working Paper 2003-2

February 2003

Managing Operational Risk in Payment, Clearing, and Settlement Systems

by

Kim McPhail

Department of Banking Operations
Bank of Canada
Ottawa, Ontario, Canada K1A 0G9
kmcphail@bankofcanada.ca

The views expressed in this paper are those of the author.
No responsibility for them should be attributed to the Bank of Canada.

Contents

Acknowledgements iv
Abstract v
Résumé vi

1. Introduction 1

2. Systemically Important Payment, Clearing, and Settlement Systems in Canada 3

3. Operational Risk and Oversight of Systemically Important PCSS 5

4. The Growing Awareness of Operational Risk 8

5. A Possible Framework for Assessing and Managing Operational Risk in PCSS 10
   - 5.1 Defining operational risk in PCSS 11
   - 5.2 Identifying operational risk in PCSS 12
   - 5.3 Assessing and measuring operational risk in PCSS 13
   - 5.4 Controlling and mitigating operational risk in PCSS 16
   - 5.5 Monitoring operational risk in PCSS 18

6. Conclusion 19

Bibliography 20

Figures 23

Appendix A: Recent Regulatory Developments with Respect to Operational Risk in Financial Institutions 26

Acknowledgements

I would like to thank colleagues at the Bank, particularly Walter Engert, Clyde Goodlet, Paul Miller, Carol Ann Northcott, and Jim Reain, for helpful comments on this paper. All remaining errors are my own.

Abstract

Awareness of operational risk has increased greatly in recent years, both at individual financial institutions and for payment, clearing, and settlement systems (PCSS). PCSS consist of networks of interconnected elements (i.e., central operators, participants, and settlement agents); operational problems at any one of the key elements have the potential to disrupt the system as a whole and negatively affect financial stability.

The author describes the key features of systemically important PCSS in Canada and the oversight role of the Bank of Canada with respect to those systems. She also describes one approach that could be used to assess and manage operational risk in Canadian PCSS.

This approach relies on a consistent definition of operational risk that can be applied across all elements of a PCSS. It uses a recent methodology adapted from the management of operational risk at individual financial institutions. This methodology, called the loss-distribution approach, assesses risk in terms of the potential outcomes of operational events owing to certain risk factors (such as systems problems, human error, process problems, and external events), their likelihood, and their frequency.

Once operational risk databases are developed that record the frequency and severity of operational events, it will be possible to estimate parts of the loss distributions for PCSS. In the meantime, qualitative analysis provided by operations experts associated with the various elements of PCSS will be important for judging the potential impact and frequency of events.

In a changing financial environment, it is hoped that this methodology could be used to supplement core aspects of operational risk management, such as sound corporate governance, internal controls, policies and procedures, knowledgeable people, and robust contingency plans.

JEL classification: E44, G21
Bank classification: Financial institutions; Payments, clearing and settlements systems

Résumé

La prise en considération du risque opérationnel s'est grandement améliorée ces dernières années tant chez les institutions financières que dans les systèmes de paiement et de règlement. Ces systèmes se composent de réseaux d'éléments interconnectés (opérateurs centraux, participants et agents de règlement), et les problèmes opérationnels associés à chacun des éléments clés peuvent perturber l'ensemble du système et avoir des retombées négatives sur la stabilité financière du pays.

Ce document débute par une description des éléments clés des principaux systèmes canadiens et un exposé du rôle de surveillance que joue la Banque du Canada dans ce domaine. Puis, l'auteure expose une méthode pouvant servir à estimer et à gérer le risque opérationnel auxquels les systèmes de règlement et de compensation sont confrontés au Canada.

L'approche en question repose sur une définition cohérente du risque opérationnel applicable aux divers éléments des systèmes de paiement et de règlement. Elle utilise une méthodologie récente inspirée du mode de gestion du risque opérationnel dans les institutions financières. Connue sous le nom d'approche de distribution des pertes, cette méthode permet d'estimer les risques en fonction, d'une part, des conséquences potentielles de situations telles que les problèmes systémiques, les erreurs humaines, le non-respect de certaines exigences juridiques procédures, certains événements externes, etc. et, d'autre part, de la probabilité et de la fréquence de ces situations.

Une fois que seront constituées les bases de données relatives au risque opérationnel, où seront consignées la fréquence et la gravité des événements d'ordre opérationnel, il sera possible d'estimer certaines parties de la distribution des pertes subies par les systèmes de paiement et de règlement. En attendant, il faudra compter sur les analyses qualitatives des experts du secteur opérationnel pour évaluer l'impact possible et la fréquence des événements affectant les divers aspects des systèmes de paiement et de règlement.

Dans l'environnement financier en pleine évolution d'aujourd'hui, on espère pouvoir mettre cette méthodologie à contribution pour compléter les éléments de base de la gestion du risque opérationnel tels que le régime de gestion des sociétés, les contrôles internes, les politiques et procédures, les compétences du personnel, les plans d'urgence.

Classification JEL : E44, G21
Classification de la Banque : Institutions financières; Systèmes de paiement, de compensation et de règlement

1. Introduction

Sound management of operational risk in systemically important payment, clearing, and settlement systems (PCSS) is important for financial stability. During the day, PCSS allow financial institutions (and, indirectly, their clients) to exchange payments that are irrevocable and final, settle securities transactions, and finalize the transfer of funds involved in foreign exchange transactions. PCSS are networks that underpin much financial and economic activity. The elements of these networks include their operators, participants, and settlement agents.[1] One PCSS may be closely linked to another, so disruptions in one may cause problems for another domestic or international system.

This paper uses recent advances in the management of operational risk at individual financial institutions to develop a unified framework that could be used to assess and manage operational risk in Canadian PCSS that are systemically important. Because PCSS consist of networks of interconnected elements, many of which are critical to the functioning of these systems as a whole, a systemic approach provides a different and more robust perspective than when operational risk is analyzed separately at each element of the network. The repercussions of the 11 September 2001 terrorist attacks in the United States illustrate these connections and the usefulness of taking an integrated approach to assess operational risk in PCSS and the management of severe operational events.

Many financial institutions are trying to move away from a methodology that examines risk in individual areas of an institution in isolation towards a method that allows for operational risk in different areas to be measured objectively (in terms of potential financial loss) and integrated across the entire institution. This paper aims to adapt this approach so that a similar unified one can be taken with PCSS. It is more difficult to apply this approach in PCSS because it is not our intent to measure the consequence of adverse operational events in PCSS in terms of financial loss but in terms of the degree of financial instability that they may cause, and this may be difficult or impossible to quantify. Hence, qualitative judgments will remain important. Nevertheless, adapting this unified approach, even if it is based mainly on judgment and estimates rather than hard data, focuses attention on the systemic aspects of operational risk in PCSS that are of most

1. The infrastructure linking these elements, such as SWIFT messaging systems and power systems, are also important to PCSS. Clients who use a financial institution to transfer funds and securities could be considered part of a more broadly defined clearing and settlement network, since they would be concerned about the operational reliability of systems. This paper, however, is limited to the narrower definition just given.

concern to central banks. Over time, as databases on operational events are built up, a more empirically focused approach will become possible.

PCSS are a key part of the financial infrastructure. Because of their critical function in the economy, PCSS must be safe, reliable, efficient, and secure. They must operate reliably at critical times of the day and without sustained periods of disruption, except in the worst possible scenarios. Serious consequences may arise due to severe disruptions at any element of a PCSS (operator, participant, or settlement agent). For example, some serious disruptions may prevent a system operator or a participant from operating from their primary site. The failure of business-continuity plans designed to allow operations to resume at an alternate site could have serious consequences. Operational problems in a PCSS may impede the control of, or even exacerbate, other types of risk (e.g., market, liquidity, or credit risk) in a way that could pose systemic risk. Participants in a system might incur significant losses. Operational problems at a participant in a PCSS could disrupt the payments and settlement activities of other financial institutions in the system in a way that they cannot anticipate or prevent. This could lead to intraday liquidity problems or end-of-day settlement delays. Severe operational problems can affect interest rates in overnight money markets. Operational problems that are extremely severe might halt the operation of a PCSS for an extended period of time, thereby preventing the exchange of payments or securities. This could have severe consequences for financial stability. Increasingly, operational disruptions in a national PCSS can have international repercussions.

The operational reliability of Canadian PCSS could affect the volume of some transactions in PCSS and, in extreme cases, the absolute willingness of economic agents, both domestic and foreign, to enter into financial transactions that ultimately rely on the settlement of Canadian-dollar assets. This could have a negative impact on the efficiency of the financial system and of the Canadian economy.

Traditionally, the management of operational risk in both financial institutions and PCSS has relied on sound corporate governance, internal controls, policies and procedures, knowledgeable people, and robust contingency plans. These will remain the foundation of operational risk management. In a rapidly changing world, however, it may be more difficult to adapt procedures quickly to reflect changes in the source of operational risk. Consequently, new tools and processes are being developed to manage operational risk that will be more forward looking. One purpose of this paper is to adapt these tools and processes so that they can supplement traditional methods of assessing and managing operational risk in PCSS.

This paper is organized as follows. Section 2 describes the key PCSS for payments, securities, and other transactions in Canada. Section 3 describes the Bank of Canada's oversight role regarding

systemically important PCSS in Canada and its link to operational risk. Section 4 explains why awareness of operational risk has increased. Section 5 describes a process that could be used to assess and manage operational risk in PCSS. It involves defining, identifying, assessing and measuring, controlling, mitigating, and monitoring risk. An example is given of how this process might be implemented. Section 6 evaluates the usefulness of this type of framework for the overall assessment of operational risk in PCSS.

2. Systemically Important Payment, Clearing, and Settlement Systems in Canada

Canada has a number of PCSS for payments, securities, and other financial instruments. Two domestic settlement systems are key: (i) the Large Value Transfer System (LVTS), owned and operated by the Canadian Payments Association (CPA), and (ii) the Debt Clearing Service (DCS), owned and operated by the Canadian Depository for Securities (CDS).[2] The CPA consists of deposit-taking institutions. In November 2001, legislation came into effect that allows life insurance companies, securities dealers, and money market mutual funds to be eligible for membership in the CPA. None of these institutions has joined the CPA to date. The CDS is a private-sector corporation owned by major Canadian chartered banks, members of the Investment Dealers Association of Canada, and the Toronto Stock Exchange. About 120 institutions, including the Bank of Canada, are members of the CDS.

The LVTS provides for the intraday exchange of large-value or time-sensitive payments. Thirteen deposit-taking institutions as well as the Bank of Canada are direct participants in the LVTS. The DCS settles Government of Canada securities, most provincial government debt, corporate debt, other long-term debt, and money market instruments. Both settlement systems are netting systems. Final settlement of the LVTS occurs at the end of the day, although the system has intra-day finality; that is, each payment that passes through the LVTS during the day is final and irrevocable. DCS also settles at the end of the day.

A collateral pool in the LVTS ensures that the system will settle at the end of the day even if the participant with the largest net debit position fails.[3] In the extremely remote possibility of multiple defaults, and if the collateral pool is not sufficient to absorb losses, the Bank of Canada guarantees settlement of the system.

---

2. For a description of the major features of the LVTS, see Dingle (1998). For a brief description of the features of the DCS, see Freedman (1999). See also the Bank of Canada Web site at http://www.bankofcanada.ca/.
3. The LVTS settles at 6:30 p.m. EST each day.

The DCS settles securities on a transaction-by-transaction basis, but nets associated payment flows. It settles these payments through the LVTS between 4 and 5 p.m. each day. The risk-proofing mechanism in the DCS ensures that it is able to settle even if the participant with the largest net debit position fails.

The LVTS and CDS (and its settlement system, the DCS) are closely linked. End-of-day settlement of payment obligations in the DCS occurs via payments made through the LVTS. The CDS is the depository for securities that provides the collateral pledged to the LVTS to support the intraday exchange of payments. Operational problems in the LVTS may therefore affect the DCS and vice versa.

In September 2002, an international foreign exchange settlement system called the Continuous Linked Settlement (CLS) Bank began operations. The CLS Bank is owned by more than sixty internationally active banks. It settles foreign exchange transactions in seven currencies, including the Canadian dollar. Because this settlement system ensures the simultaneous final settlement of both sides of a foreign exchange transaction, it will greatly reduce foreign exchange settlement risk. To accommodate the window of time during which settlement occurs, the LVTS opens at 1 a.m. for payments processing, rather than its previous opening time of 8 a.m. The DCS hours have been extended accordingly.[4]

The CLS Bank concentrates operational risk because its safe operation requires that payments in domestic payment systems in seven different countries be delivered reliably and within a tight time frame. Even short-term operational problems in the LVTS, DCS, or at a Canadian participant in the CLS Bank have the potential to create significant consequences for CLS Bank participants. Canadian financial institutions involved in the settlement of CLS Bank transactions are expected to have reliable systems and procedures and knowledgeable personnel to ensure that payments can be made on time. To address the risk that CLS Bank payments could be disrupted, the Bank of Canada has put robust backup measures in place to ensure that payments can be delivered to the CLS Bank within its time-critical window even if there are operational failures in the LVTS or at one of the CLS Bank's Canadian participants.

The Bank of Canada is an important element of Canada's PCSS because of the essential services it provides to these systems. This function is in addition to its role as a participant in these systems and as an overseer of systemically important PCSS. The Bank is the "banker" for the DCS and for the CLS Bank's Canadian-dollar operations. It provides accounts for the DCS and the CLS Bank, receives payments due to them, and sends out payments on behalf of these systems. The Bank is

4. For more on the CLS Bank, see Miller and Northcott (2002a, b).

also the settlement agent for the LVTS. This settlement occurs at the end of each day through transfers of funds in settlement accounts of LVTS participants at the Bank of Canada. The Bank provides secured advances and collateral administration services to direct participants in the LVTS in support of their daily operations. The Bank provides liquidity to system participants. It also provides contingency facilities for certain systems in some circumstances, such as those related to the CLS Bank that were previously described. Given these critical functions, operational problems at the Bank of Canada could impede the normal operation, or delay settlement, of the LVTS, DCS, or the CLS Bank. Therefore, robust contingency arrangements and escalation procedures are in place at the Bank to deal with any operational difficulties that could arise.

3. Operational Risk and Oversight of Systemically Important PCSS

The Payment Clearing and Settlement Act (PCSA) gives responsibility for formal oversight of systemically important PCSS in Canada to the Bank of Canada.[5] The LVTS, DCS, and CLS Bank have been designated under the Act and are subject to oversight by the Bank. In 1997, the Bank issued *Guideline Related to Bank of Canada Oversight Activities under the Payment Clearing and Settlement Act* (Bank of Canada 1997). An updated guideline was issued in November 2002 to reflect recent work of the Bank for International Settlements' (BIS) Committee on Payment and Settlement Systems (CPSS), composed of payments experts from the G-10 countries, and the work of the International Organization of Securities Commissions (IOSCO).

The Bank of Canada's guideline sets out the minimum standards that designated systems are expected to meet to adequately control systemic risk. The minimum standards incorporate those set out in the "Lamfalussy Report" published by the BIS in 1990 (BIS 1990). They are consistent with the CPSS's more recent publication, *Core Principles for Systemically Important Payment Systems* (BIS 2001a). They also satisfy the joint CPSS/IOSCO study, *Recommendations for Securities Settlement Systems* (CPSS/IOSCO 2001). These reports and the Bank of Canada's guideline emphasize the importance of managing credit, liquidity, legal, and operational risk in PCSS. Under the PCSA, the Bank of Canada oversees the Canadian-dollar operations of the CLS Bank and works with other central banks whose currencies are settled by the CLS Bank. The Federal Reserve has the lead oversight responsibility for the CLS Bank.

5. For a brief description of the features of this legislation, see Goodlet (1997) and Freedman (1999).

More specifically, while the CPA and CDS have primary responsibility for managing operational risk in the LVTS and DCS, the Bank's guideline requires designated systems "to ensure the operational reliability of technical systems and the availability of backup facilities capable of completing daily processing requirements." Changes to the rules affecting the LVTS and DCS are assessed by the Bank for their potential to pose systemic risk and for conforming to the Bank's guideline for designated PCSS.

The Office of the Superintendent of Financial Institutions (OSFI) is responsible for the regulation of federally chartered financial institutions. As part of its supervisory activities, the OSFI requires these institutions to have sound principles and practices for operational risk management, including appropriate contingency plans. The PCSA does not give the Bank oversight responsibilities for individual financial institutions that participate in designated PCSS, except to the extent that problems at an institution are *directly* related to its participation in the system.[6] PCSS operators are expected to monitor participants' compliance with the system's operational rules and guidelines. They are also expected to assess the adequacy of participants' backup capabilities that allow them to restore operations quickly in the event of disruptions to their primary processing operations. The Bank of Canada, in turn, assesses the adequacy of technical competency standards and the compliance activities of these systems to satisfy itself that sources of systemic risk are contained. In the case of a participant experiencing frequent operational problems that affected PCSS, the Bank would draw the OSFI's attention to the problem. In extreme situations, where the Governor of the Bank judged that systemic risk in PCSS was not being adequately controlled, the Governor could issue directives to the system operators or, in certain circumstances, to the participants in a designated system.

The Bank relies on external audits of the LVTS and DCS to determine the effectiveness of internal controls in achieving the operational integrity of these systems. The Bank can also require audits of particular aspects of the LVTS and DCS that are of concern to it as a result of its oversight responsibilities for systemic risk. Certain essential operations provided by the Bank to support the LVTS may be reviewed as part of this external audit.

The CDS provides a considerable amount of information regarding its management of operational risk on its Web site (http://www.cds.ca) and through various publications. It provides information about the operational reliability of its system relative to performance objectives. Its *Report on*

6. For example, the Bank has no jurisdiction over a participant's capital adequacy, the management of its investments, or its relations with its customers, even though these may affect its solvency and hence its ability to participate in PCSS.

Internal Controls and Safeguards sets out its overall risk-management objectives, controls, and practices, and includes the annual report of its external auditors.

In June 2000, the International Monetary Fund (IMF) assessed the LVTS and found it to be fully compliant with the CPSS's *Core Principles for Systemically Important Payment Systems* (BIS 2001a; IMF 2000). The CPA's Web site (http://www.cdnpay.ca/eng/home-e.htm) also reports on a self-assessment with the Core Principles and finds the LVTS to be fully compliant.

The Bank of Canada monitors the LVTS and DCS on an ongoing basis for intraday operational problems and end-of-day settlement delays. It notes whether these were generated by problems at a system participant, by the central system operator, or by the Bank of Canada. Any necessary follow-up action is taken. The Canadian-dollar operations of the CLS Bank are also monitored closely.

Over the past decade, much of the attention of overseers of PCSS has focused on the design of systems to control liquidity and credit risk. Their attention is turning increasingly, in Canada and abroad, to operational risk. In the past, operational reliability of PCSS has emphasized the ability of these systems to settle without significant delay at the end of the day. More attention is now being given to the intra-day reliability of these systems.

For example, a recent BIS/IOSCO report (BIS/IOSCO 2001) on securities settlement systems expands on expectations of operational reliability for major securities settlement systems. The report indicates that system operators should have a process for identifying and managing operational risk, whether this risk arises from the central system operator or from participants of the system. It sets out a series of questions that can be used to assess operational risk (and other risks) in securities settlement systems as well as assess the use of well-established methods for determining compliance with operational risk standards (e.g., corporate governance, policies and procedures, and contingency arrangements). An assessment of the intraday reliability of these systems requires operators to consider how long it takes to recover operations through backup systems, how often these are tested, and whether these procedures provide for the preservation of all transactions data. It is also important for system operators to keep track of how many times a year a key system has failed, how long it took to resume processing, and whether any transactions data were lost. The overseers in each country are expected to evaluate the compliance of securities settlement systems with these procedures.

4. The Growing Awareness of Operational Risk

Awareness of operational risk has increased sharply in recent years, partly due to well-publicized, very sizable losses suffered by a number of large financial institutions over the past decade as a result of weaknesses in internal controls. There is a growing recognition that, although the likelihood is small, the financial consequences of such events could be extremely damaging.

The effect of operational risk on the financial infrastructure, including PCSS, has also gained attention. A severe operational problem within a financial institution can create problems for important parts of the financial system architecture. A prominent example of such an event is that of the Bank of New York (BONY), because of the key role it plays in clearing U.S.-dollar securities. In 1985, a 28-hour computer malfunction prevented BONY from carrying out its securities-related activities. As a result, BONY needed to borrow a record amount—more than $20 billion—from the Federal Reserve's discount window. Other financial institutions were left with a corresponding excess of cash. Their efforts to dispose of this surplus temporarily drove the federal funds rate down by about 300 basis points.[7] Problems at BONY during the events following 11 September 2001 also contributed to extreme liquidity disruptions and problems in securities markets in the United States.

In 1990, a fire in New York left a number of buildings in lower Manhattan, including that of the Federal Reserve Bank of New York, without power for six days. While financial transactions continued to be processed, severe demands were placed on operations and backup facilities.[8]

Operational risk in the financial infrastructure can also spill over to international markets. In April 2000, a software problem caused trading on the London Stock Exchange (LSE) to stop for almost eight hours. The London International Futures Exchange, which uses spot prices obtained from the LSE to value futures contracts, was also affected. The inability to adjust U.K. portfolios was reported to have caused a number of investors to sell European shares, and prices on European exchanges fell.[9]

The realization of operational risk in PCSS may result in market, liquidity, and credit risk problems. The events following the terrorist attacks of 11 September 2001 affected the entire financial infrastructure in the United States and parts of the infrastructure in Canada and other countries. Large-value payment systems around the world remained open during that period and

7. *Wall Street Journal*, 25 November 1985.
8. Corrigan (1996).
9. *Wall Street Journal*, 6 April 2000.

the financial architecture functioned remarkably well under the circumstances. Nevertheless, the settlement of bond transactions in the United States was severely disrupted and dislocations in U.S. payment systems contributed to severe liquidity problems at some institutions. Major stock exchanges in the United States and Canada closed. The two largest electronic interbank trading systems for foreign exchange transactions, Reuters and EBS, also closed for a short time due to an overload of backup systems. In Canada, concern by domestic financial institutions that they might not receive U.S. funds owing to them in a timely fashion (because of potential disruptions in U.S. payment systems) altered the flow of payments in the LVTS.

The events of 11 September have emphasized the importance of documented, validated, and tested contingency plans to deal with extreme events. Around the world, operators of PCSS are re-examining whether contingency plans are robust enough to deal with the consequences of extreme disruptions of one or more of the critical elements of PCSS.

Operational risk management has gained prominence for other reasons. Change in the financial sector globally has been rapid in the past decade and it will continue in the future. Examples include globalization (e.g., the CLS Bank), disintermediation, and the increasing complexity of financial instruments. Growing linkages between systems, such as those between large-value payment systems in currencies settled by the CLS Bank, make the consequences of operational events in one element of these networks more serious and widespread. In North America, large-value payment systems and some securities settlement systems are moving towards 24-hour availability. Technological advances are leading to increasing economies of scale and scope that influence many aspects of PCSS. They may reduce the optimal number of direct participants in PCSS and, indeed, the efficient number of PCSS. As these trends evolve, concentration may increase and this tends to make more severe the consequences of operational disruptions at one of the key elements of the financial infrastructure. This may require PCSS to invest more resources to reduce the financial system's vulnerability to this type of shock.

Technological advances can also shift the composition of operational risk. New technologies are often adopted because of cost considerations rather than because of any expected reduction in risk. Although advancing technology allows for more straight-through processing and a reduction in manual intervention, more sophisticated technology may make it more difficult to identify the nature of operational problems and may take much longer to resolve them when they occur. Moreover, when these systems fail, it may be far more difficult to rely on manual backup to keep operations going than for smaller, less complex systems. Disruptions in these more efficient, integrated systems should occur much less frequently, but their consequences may be more severe.

It will likely become increasingly important for many payments and financial instruments to be delivered promptly at specific times of day. The time-sensitive requirements for payments to the CLS Bank are a primary example. As this time-criticality grows in importance, it places a much greater burden on the operational reliability of all elements of PCSS—operators, participants, and settlement agents.

These changes increase the complexity of operational risk management. As stated earlier, traditional elements of corporate governance, strong internal controls, policies and procedures, and knowledgeable people will remain core aspects of operational risk management. However, the rapidly evolving environment raises the question of whether traditional approaches to operational risk management can be supplemented by additional measures. Owing to rapid change, some operational risk mitigants, such as policies and procedures, become less effective because they are difficult to adjust quickly and to keep up to date. External audits tend to focus on how well risk-management objectives were met in the recent past, and may provide less valuable information about how effective operational risk management will be in the changing environment of the future.

To date, operational risk measurement has relied largely on a "qualitative" and "disaggregated" approach. Building on advances in modelling credit and market risks, however, many large financial institutions are now starting to develop "quantitative" models that integrate the assessment of operational risk across a financial institution. These models could supplement qualitative approaches for measuring and managing operational risk. The objective is to determine whether quantitative approaches can add consistency, objectivity, and rigour in managing operational risk across all business lines of a financial institution. Section 5 describes how one of these recent approaches could be adapted to analyze operational risk in PCSS.

5. A Possible Framework for Assessing and Managing Operational Risk in PCSS

This section focuses on the systemic aspect of operational risk in PCSS, rather than on the consequences of operational events for individual participants in PCSS. This systemic perspective may, therefore, differ from that of a participant in a PCSS, for example.

An approach is described that could be used to assess and manage operational risk in PCSS. It borrows heavily from the framework set up by the BIS to address the management of operational risk at individual financial institutions. Appendix A summarizes much of the recent work done by the BIS in operational risk management at individual financial institutions.

Many elements of operational risk can be in common at financial institutions or in PCSS, but some elements differ. A financial institution is concerned with the effects of risk on its own institution. PCSS, however, are interconnected networks. Each participant in a PCSS will have its own risk-management strategy and practices that it has developed for its own internal risk-management purposes. Externalities, however, may tend to limit the degree to which one element (e.g., a participant) of a PCSS looks beyond the effects of operational events on its own business and considers its systemic consequences for PCSS. It is therefore important that the central operator of a PCSS sets clear standards that participants must meet to prevent or limit the consequences of disruptions in their own operations for PCSS as a whole.

In terms of the methodology that we propose, the model for managing operational risk in PCSS involves defining, identifying, assessing and measuring, controlling and mitigating, and monitoring operational risk. This methodology is recommended in virtually all recent publications (including those of the BIS).

5.1 Defining operational risk in PCSS

Following the approach taken by the BIS[10] for individual financial institutions, operational risk in PCSS is defined as follows:

> The risk resulting from inadequate or failed internal processes, systems, human error, or from external events related to any element of payment, clearing, and settlement systems.

In describing the consequences of operational risk in PCSS, the focus will be on the potential for financial instability when serious problems arise in these systems. The focus of this definition on the causes of operational risk (these are also called risk factors) is useful. It provides a direct link between the causes of operational risk and consequences for PCSS and, therefore, for financial stability, rather than emphasizing the multitude of operational events that are the symptoms of operational risk. Note that credit-related factors such as the default of a participant are not considered as one of the causes that can create operational risk.

Many causes of operational disruptions are internal to one or more elements of PCSS (participants, operators, and settlement agents). For example, systems problems at an LVTS participant may alter the payment activity of other participants and, thus, the payment system as a whole. Similarly, a problem caused by human error at the central operator might cause a lengthy intraday LVTS outage that disrupts the payment activities of all participants. This could

10. The BIS defines operational risk for a financial institution as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events" (BIS 2002a).

significantly delay the settlement of the DCS. Conversely, a lengthy delay in settlement of the DCS could delay settlement of the LVTS. In such a case, the finality and certainty of settlement is not at risk because of the design and risk controls of the system. Since the CLS Bank is operational, however, the consequences of late settlement of the LVTS have intensified, because it takes several hours for the LVTS and participants to adjust their computer systems to process time-critical CLS Bank-related payments early the next morning, when CLS payment traffic is heavy. Other operational risk factors that can contribute to financial instability may be external. These could include natural disasters (earthquake, fire, flood) at a participant, settlement agent, or operator of a PCSS.[11] The terrorist attacks of 11 September 2001 are an example of an external risk factor that affected all elements of PCSS in the United States and many elements of the financial infrastructure in Canada and abroad.

5.2 Identifying operational risk in PCSS

The definition of operational risk has already set out the risk factors for PCSS. It may, in fact, be easier to identify operational risk in PCSS than in financial institutions. In financial institutions, the dividing line between credit risk, for example, and operational risk may not be clear.[12] In PCSS, these issues do not pose problems, since the primary focus of the operational risk-management framework for PCSS is related to the effect of risk on financial stability.

In identifying operational risk in PCSS, it helps to identify the risk factors that are most important for preserving the smooth functioning of PCSS (e.g., key systems, processes, and resources). This helps to set priorities when it comes to measuring, analyzing, and managing operational risk as well as establishing contingency measures, such as business-continuity plans, to deal with extreme events. This assessment can be made by operational experts in PCSS who are aware of the most critical elements of processes, systems, and skills required for successful operations. These experts may come from the operators of PCSS, their participants, or their settlement agents. These experts are also well-placed to consider how changes to business procedures or functions may reduce the level of operational risk. An environmental scan can help to identify potential changes in external risk factors that originate outside PCSS.

The consequences of adverse operational events in PCSS for financial instability are extremely difficult, and may be impossible, to quantify. The judgment of operational experts can be helpful in developing a consensus on values that can be used to create an index of "financial instability."

11. See Corrigan (1996).
12. For example, institutions may vary in allocating losses due to breaches of credit limits to credit risk or to operational risk.

Experts can benchmark the values of this index by assigning a number from 0 to 7, for example, to measure the consequences of specific operational events in PCSS. Thus, a one-hour settlement delay of the DCS might receive a value of 2 and a lengthy intraday outage in the LVTS might receive a value of 3. A failure to make CLS Bank-related payments might receive a value of 4. With a few such benchmarks, as operational events occur, it would be easier to rank less arbitrarily their effects on financial instability by considering their consequences relative to the benchmarks that had already been established. In effect, this approach to identifying operational risk is similar to an internal risk assessment and also involves qualitative scenario analysis. This scenario analysis allows experts to assess the consequences of extreme events that have a very low likelihood of occurring, but it adds some rigour by attempting to compare the severity of different events on a consistent basis. This is useful to identify areas of risk and to develop appropriate contingency measures to manage these types of events should they occur.

5.3 Assessing and measuring operational risk in PCSS

One way to implement this methodology for measuring operational risk in PCSS would be to adapt the loss-distribution approach put forward by the Basel Committee to measure operational risk in a financial institution. The loss distribution captures three elements of risk: the range of outcomes that may be associated with a single risk factor, the likelihood of each of those outcomes, and the frequency with which one can expect this risk factor to occur over a particular horizon. The first two elements are captured in the loss-severity distribution (LSD). The third is captured in a frequency distribution. The LSD and frequency distribution are blended together to form the loss distribution. When establishing the loss distribution, it would likely be more effective to base it on the "residual" risk that remains after existing internal controls and other risk-mitigation measures are taken into account.[13]

A single risk factor (such as a systems problem) that affects a PCSS can generally be associated with a continuum of consequences, depending on the circumstances that exist when the problem occurs and the duration of the problem. In other words, the consequences are almost always uncertain. Associated with each of these potential outcomes is a likelihood (or probability). This relationship between possible consequences in terms of the index of financial instability (measured along the horizontal axis) and their associated likelihoods (along the vertical axis) is the LSD

13. For some purposes, however, the loss distribution *before* all risk mitigants are considered will be relevant to a central bank. For example, the Bank of Canada provides certain contingency arrangements to PCSS and their participants in some situations. The Bank would also be interested in the likelihood, potential consequences, and frequency of operational events before taking into account the operational support provided as a last resort by the Bank.

shown in Figure 1. The LSD measures the range of potential outcomes of a *single* occurrence of a risk factor and says nothing about the *frequency* with which this risk factor could occur.

The LSD is not a complete measurement of operational risk. One must also assess the frequency of the risk factor over a given time horizon (e.g., one year). In almost all cases, the frequency of a risk factor is also uncertain. This uncertainty is captured by specifying a frequency distribution for the risk factor (Figure 2). This distribution describes the number of times a risk factor could occur over a particular horizon together with an associated probability. A frequency distribution often has the symmetric shape shown in Figure 2. It is generally assumed to be independent of the LSD.[14]

Information about the LSD and frequency distributions is valuable in itself. When the LSD and frequency distribution are combined, the result is the loss distribution, which could have a shape like that shown in Figure 3. This distribution can be viewed as the complete risk profile of a risk factor. Aggregating across all risk factors provides an overall loss distribution or operational risk profile for a PCSS.

Combining the LSD and frequency distributions to obtain a loss distribution is not a simple process. An analytical loss distribution cannot typically be calculated and, in general, the simplest way to calculate the loss distribution would be to use a numerical method such as a Monte Carlo simulation.[15] The loss distribution incorporates uncertainty in both the consequences of a single risk factor and in the frequency of the risk factor.

To illustrate how the loss-distribution approach might be implemented in practice, consider the risk associated with systems, human error, or process problems at participants of a PCSS. A group of operational experts in PCSS would already have established an index of financial instability as described in section 5.2. The first step in establishing the loss distribution would be to develop a view on the LSD.

If a database that recorded past operational events existed, it could be used to assess part of the LSD. The database would contain information on each operational event at participants and its consequences (i.e., the value of the financial instability index). For example, if the database indicated that, 75 per cent of the time, operational events at participants had an effect on the index

14. If we consider, for example, intraday outages of the LVTS, this statistical independence means (loosely speaking) that the range of consequences we expect to see for a single outage is not influenced by the number of outages that occur. One can think of a few counter-examples where this statistical independence is not true. However, calculation of the loss distribution becomes much more complex if this assumption is dropped.

15. See Frachot, Georges, and Roncalli (2001).

equal to 2, the likelihood associated with a consequence of 2 would be 0.75. If events that had a consequence of 5 occurred 0.5 per cent of the time, the likelihood associated with a consequence of 5 would be 0.005. In the absence of such data, operational experts could use their expertise to judge what these likelihoods were, based on their assessment of factors such as the time of day that a problem occurred and the duration of the problem. For example, they could consider the scenarios that would give rise to a consequence of 5, and use their judgment about the conditions that would be required to generate those scenarios to estimate the associated likelihood.

The next step would be to estimate the frequency distribution. If a database on operational events existed, the frequency of operational events at participants of PCSS would be available. One could look at how often problems at participants occurred and how variable those events were from month to month, to estimate the mean and variance of the frequency distribution. In the absence of hard data, operational experts could use their general knowledge of how frequent and variable operational events at participants had been in the past to form a view of this distribution. Monte Carlo simulations could then be used to generate a loss distribution that combined the LSD and frequency distribution.

The introduction of CLS operations provides an example of how a loss distribution can shift as other parts of the financial infrastructure evolve. The CLS would initially affect the LSD associated with operational problems of participants and could also affect the frequency distribution during the testing phase, before the CLS began live operations.

During the testing phase, the frequency distribution might shift due to inexperience with making CLS Bank payments during overnight hours. This might make problems at some participants more frequent and possibly more variable until experience was gained. The CLS Bank maintained a three-month trial period during which time participants had the opportunity to ensure that their systems and processes could meet high standards. During this period, and before the start-up of live operations in September 2002, each CLS settlement member was formally assessed by the CLS Bank for its ability to meet high operational standards. By the time the CLS began live operations, one would expect that the frequency distribution would have shifted back to close to its original profile.

The LSD would certainly potentially be affected once the CLS process was introduced because failure to make payments to the CLS Bank when due could have fairly serious consequences. Thus, compared with the period prior to the CLS start-up, the right-hand tail of the LSD would shift up. Indeed, it was the assessment of the Bank of Canada that the additional risk of these relatively severe consequences should be reduced by putting in place additional contingency measures that would allow participants to make payments to the CLS Bank even if their own

operations failed. These contingency arrangements, which are not intended to substitute for participants' own backup procedures but rather for use as a last resort, would shift the loss distribution back down towards its initial level. Figure 4 illustrates how the loss distribution might have shifted just before the introduction of the CLS and how it was brought back to an acceptable profile.

In many ways, the loss-distribution approach is similar to the qualitative scorecards that are frequently used in the risk literature. The scorecard approach typically assigns low, medium, or high likelihoods to problems in a business line or activity and low, medium, or high consequences associated with those problems. The scorecard approach blends a single estimate of the likelihood of an event and its consequences to form one summary measure of risk. The overall risk is then mapped into the cell of a matrix that best captures these two aspects. Figure 5 illustrates the scorecard approach with the circle in the bottom right-hand cell of the risk matrix.

The loss distribution also estimates the likelihood and consequences of an activity or business line, but it recognizes that consequences are uncertain and *each* potential consequence is associated with a given probability (Figure 5). Thus, this approach provides a more disaggregated estimate about the risk profile associated with operational risk in PCSS and ensures that *every* point of the distribution falls within acceptable risk tolerances. The point estimate associated with a scorecard could be viewed as one way of aggregating all the information captured in the loss distribution.

5.4 Controlling and mitigating operational risk in PCSS

Loss distributions are endogenous. Recall that loss distribution was defined as the relationship between cause and consequences after all internal controls and other risk mitigants are taken into account. The shape of the distribution will therefore depend on how risk is managed. For example, if effective risk mitigants are put in place to deal with potentially severe outcomes, the right-hand tail of the distribution will shift down.

Once operational risk has been measured, it must be analyzed to determine what areas of the distribution fall within acceptable risk tolerances and where risk tolerances are exceeded. By adopting an integrated approach across all elements of PCSS, one can then identify where gaps exist along all possible outcomes that originate from any element of PCSS (system operator, participant, or settlement agent) and prioritize how to address them. Indeed, even when risk falls within acceptable tolerances, there is a good case for reducing it when the net benefits are positive. Risk management should address not only current gaps in risk exposures but also projections of future gaps that may arise as the financial environment and domestic and

international PCSS evolve. A good example is the rigorous analysis, well in advance of the start-up of operations, designed to ensure that the CLS Bank, its participants, and national payment systems met operational standards and had robust contingency arrangements.

In PCSS, when gaps exist between actual risk levels and tolerances, there are a number of options for addressing them, though fewer than for an individual financial institution. A financial institution can exit a business, outsource certain functions, insure or hedge some risks in the market, or invest in stronger risk mitigants. It can also choose to accept a greater degree of operational risk and hold more capital to protect itself from adverse operational events that cause financial losses.[16] Ultimately, in the case of "catastrophic" operational events (e.g., those that affected Barings Bank in 1995), in the absence of sufficient capital, a financial institution would become insolvent.

On a national scale, "exiting the business" is not an option for PCSS, because they are an essential part of the financial infrastructure and are often unique. The concept of economic capital is not meaningful in a PCSS as a buffer for operational events. Given the requirement that PCSS must function effectively, the main tool for managing operational risk in PCSS is to invest resources in each element of these networks to prevent severe operational events, or to develop contingency measures that can be used to mitigate their consequences if these events occur. Thus, a PCSS that manages operational risk effectively might have a loss distribution that is much more tightly concentrated around less-severe outcomes than that of a financial institution.

For a PCSS, some causes of operational risk are controllable. The likelihood of some risk factors may be reduced. For example, training can reduce the likelihood of human error. Internal controls can provide a buffer between human or system errors and potentially serious consequences. Risk mitigants such as robust and regularly tested business-continuity plans can decrease the consequence of an event (often due to external, uncontrollable events) that renders operations impossible at a primary site, by allowing them to resume quickly at a backup site. Emergency-response plans can be used to deal with events that are totally unpredictable and that cannot be handled fully by existing business-continuity planning. Each element of a PCSS has options for preventing or mitigating risk. Often, however, the way in which these elements manage events in an integrated fashion determines how successfully a PCSS can cope with severe operational stress. Thus, coordinated planning and testing of contingency measures by the critical elements of PCSS can be very helpful.

16. Regulatory requirements, however, ensure that financial institutions hold a minimum level of capital.

Figure 6 shows one way to think about the loss distribution for PCSS. Operational problems at PCSS participants, at the operators of the systems, or at their settlement agent that have an effect less than FI_1 have a minimal impact on financial stability and would not be an important concern. At the other extreme, the costs of putting in place measures to prevent events that have consequences in excess of FI_2 might be exorbitant. Indeed, because operational risk can never be driven to zero, it might be impossible to eliminate this residual risk. Rather, if such extremely remote and unpredictable situations ever occurred, their effects would be managed as events unfolded via emergency-response plans and any other measures that could be taken at the time to mitigate the situation.

Thus, the focus for day-to-day sound operational risk management would be on controlling potential outcomes that fell between FI_1 and FI_2 and ensuring that the likelihoods associated with these outcomes were within acceptable risk tolerances. Beyond FI_1, the degree of financial instability caused by operational problems in PCSS would become more and more disruptive and a greater concern. Thus, one would like to see that, as these potential consequences increased, risk management ensured that the associated likelihoods declined and did not exceed acceptable tolerances.

5.5 Monitoring operational risk in PCSS

PCSS are more and more dependent on information systems. Technologically effective, up-to-date, and user-friendly management information systems (MIS) are necessary so that systematic, comprehensive, objective, timely, and accurate information related to operational risk can be generated, analyzed, summarized, and reported. The building of databases on operational events should be a priority.

By building a database with a history of operational events, changing sources of operational risk are easier to detect. The judgment of experts in the field will always remain important for assessing operational risk, particularly for extreme events that occur infrequently (or may not yet have occurred). As changes occur in the financial environment, as technological innovations continue, and the complexity of financial instruments and of PCSS themselves grow, the risk factors that give rise to operational risk in PCSS are likely to evolve. By monitoring these changes using data from the database and by projecting future changes, one can assess the effect that the changes will have on the loss distribution. These may indicate that the loss distribution for events with relatively severe consequences in PCSS has shifted upward and that stronger risk mitigants are needed to bring the risk profile back to acceptable tolerances. An MIS can be used to identify coincident indicators of operational vulnerabilities and to commence development of leading

indicators of future operational problems. These systems can also be used to establish performance indicators and to evaluate how operations perform relative to these metrics. Periodic reports can be provided that aggregate this information.

6. Conclusion

Awareness of operational risk in PCSS is growing, in Canada and abroad. As PCSS become more interconnected, successful management of operational risk is growing more important and more complex.

The framework described above provides a way in which operational risk in PCSS could be assessed and managed in systemically important Canadian PCSS. PCSS in Canada are owned and operated by the private sector. Thus, it is their responsibility to ensure that risk brought to these systems by their operators and participants is managed effectively. And, because of the critical role the Bank of Canada plays in these systems, risk must also be well-managed at the Bank.

In addition to its oversight responsibility, the Bank may be asked to provide operational assistance to PCSS or their participants in the event of severe operational disruptions. It is important that participants and the operators of these systems have in place effective operational risk-management standards and practices that prevent excessive reliance on the Bank for operational assistance. At the same time, in the case of extreme events, such as the terrorist attacks of 11 September 2001, there is a need for coordination between the Bank and other key elements of PCSS.

The framework described in this paper could provide a unified and systemic perspective on operational risk in PCSS and a means of assessing whether operational risk in these systems is managed in a way that promotes financial stability.

Bibliography

Anonymous. 1998. *Operational Risk and Financial Institutions*. Risk Books.

Anonymous. 2000. "Operational Risk: A Special Report." *Risk* (November): S1–S40.

Bank for International Settlements (BIS). 1990. *Report of the Committee on Interbank Netting Schemes of the Central Banks of the Group of Ten Countries* (Lamfalussy Report). Committee on Payments and Settlements Systems. Publication No. 4, November.

———.1998a. *Framework for Internal Control Systems in Banking Organizations*. Basel Committee Publication No. 40, September.

———. 1998b. *Enhancing Bank Transparency*. Basel Committee Publication No. 41, September.

———. 1998c. *Operational Risk Management*. Basel Committee Publication No. 42, November.

———. 1999. *A New Capital Adequacy Framework*. Basel Committee Publication No. 50, November.

———. 2000. *A New Capital Adequacy Framework: Pillar 3—Market Discipline*. Consultative Paper. Basel Committee Publication No. 65, November.

———. 2001a. *Core Principles for Systemically Important Payment Systems*. Committee on Payment and Settlement Systems, January.

———. 2001b. *The New Basel Capital Accord*. Consultative Document. Basel Committee on Banking Supervision, January.

———. 2001c. *Operational Risk: Supporting Document to the New Basel Capital Accord*. Consultative Document. Basel Committee on Banking Supervision, January.

———. 2001d. *The New Basel Capital Accord: An Explanatory Note*. Secretariat of the Basel Committee on Banking Supervision, January.

———. 2001e. *Public Disclosures by Banks: Results of the 1999 Disclosure Survey*. Basel Committee Publication No. 80, April.

———. 2001f. *Regulatory Treatment of Operational Risk*. Basel Committee Publication, Working Paper No. 8, September.

———. 2001g. *Sound Practices for the Management and Supervision of Operational Risk*. Basel Committee Publication No. 86, December.

———. 2002a. *Sound Practices for the Management and Supervision of Operational Risk*. Basel Committee Publication, No. 91, July.

———. 2002b. *Basel Accord Reaches Agreement on New Capital Accord Issues*. 10 July.

——— and International Organization of Securities Commissions (IOSCO). 2001. *Recommendations for Securities Settlement Systems*. CPSS Publication No. 46, November.

Bank of Canada. 1997. *Guideline Related to Bank of Canada Oversight Activities under the Payment Clearing and Settlement Act*. December.

Bank of Canada. 2000. *Annual Report*. Ottawa: Bank of Canada.

British Bankers Association and Coopers & Lybrand. 1997. *Operational Risk Management Survey*. May.

Chorafas, D.N. 2001. *Managing Operational Risk: Risk Reduction Strategies for Investment and Commercial Banks*. London: Euromoney Books.

Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commissions. 2001. *Recommendations for Securities Settlement Systems*. November.

Corrigan, E.G. 1996. "Payments, Clearance and Settlement Systems: The Systemic Risk Connection." Symposium on Risk Reduction in Payments, Clearance and Settlement Systems, 25 and 26 January. New York.

Dingle, J. 1998. "The LVTS—Canada's Large-Value Transfer System." *Bank of Canada Review* (Autumn): 39–55.

Federal Reserve Bank of Chicago. 2001. *An Examiner's View of Operational Risk*. Available at http://www.chicagofed.org/bankinforeg/bankregulation/archives/opsrisk.cfm.

Frachot, A., P. Georges, and T. Roncalli. 2001. *Loss Distribution Approach for Operational Risk*. Manuscript. Groupe de Recherche Operationnelle, Credit Lyonnais, France. April. http://gro.creditlyonnais.fr/content/wp/lda.pdf.

Freedman, C. 1999. *The Regulation of Central Securities Depositories and the Linkages between CSDs and Large-Value Payment Systems*. Technical Report No. 87. Ottawa: Bank of Canada.

Frowen, S.F., R. Pringle, and B. Weller (editors). 2000. *Risk Management for Central Bankers*. London: Central Bank Publications.

Goodlet, C. 1997. "Clearing and Settlement Systems." *Bank of Canada Review* (Autumn): 9–64.

Hussain, A. 2000. *Managing Operational Risk in Financial Markets*. Oxford: Butterworth Heinemann.

International Monetary Fund (IMF). 2000. *Report on the Observance of Standards and Codes (ROSC)*. Canada. IV. Payment Systems. June.

King, J.L. 2001. *Operational Risk: Measurement and Modeling*. Chichester: John Wiley & Sons Ltd.

Lawrence, M. 2000. "Marking the Cards at ANZ." *Risk* (November): S8–S12.

Marshall, C.L. 2001. *Measuring and Managing Operational Risks in Financial Institutions*. Toronto: John Wiley and Sons Pte Ltd.

Miller, P. and C.A. Northcott. 2002a. "CLS Bank: Managing Foreign Exchange Settlement Risk." *Bank of Canada Review* (Autumn): 13–25.

———. 2002b. "The CLS Bank: Managing Risk in Foreign Exchange Settlements." *Financial System Review* 41–44. Ottawa: Bank of Canada.

Pricewaterhouse Coopers. 1999. "Operational Risk Management Survey—Executive Summary." November.

Wall Street Journal. 1985. "A Computer Snafu Snarls the Handling of Treasury Issues—Bank of New York's Problem Takes Over a Day to Fix, Platinum Futures Bid Up." 25 November.

Wall Street Journal. 2000. "Computer Snag Halts London Market 8 Hours—Second Breakdown in the Week Comes as the Exchange Faces Tough Challenges." 6 April.

Figure 1: Loss-Severity Distribution (LSD) of a Single Risk Factor

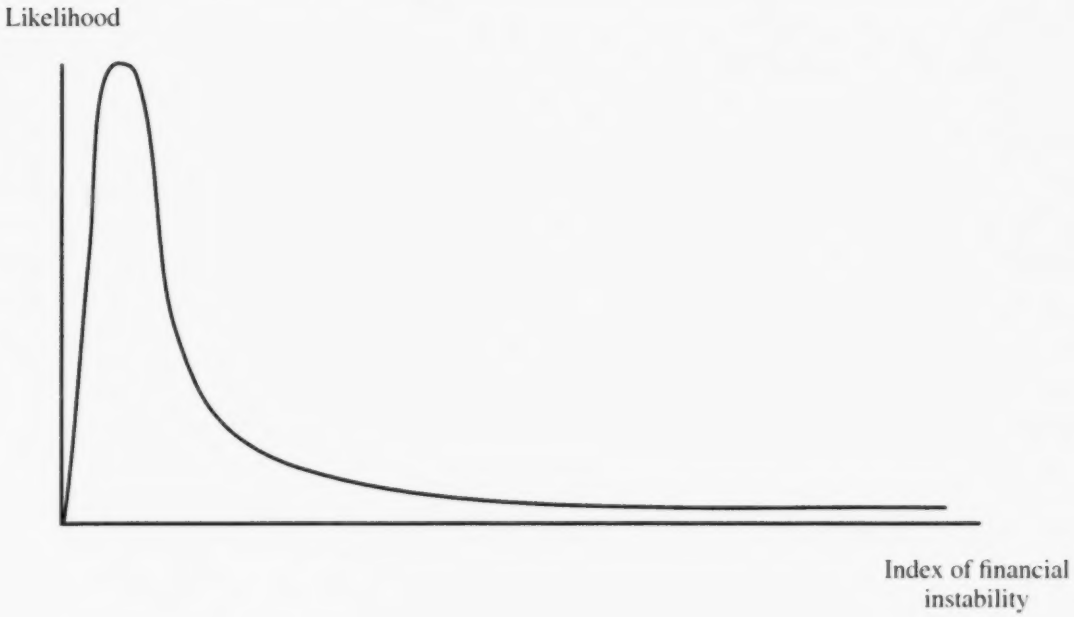


Figure 2: Frequency Distribution of a Risk Factor

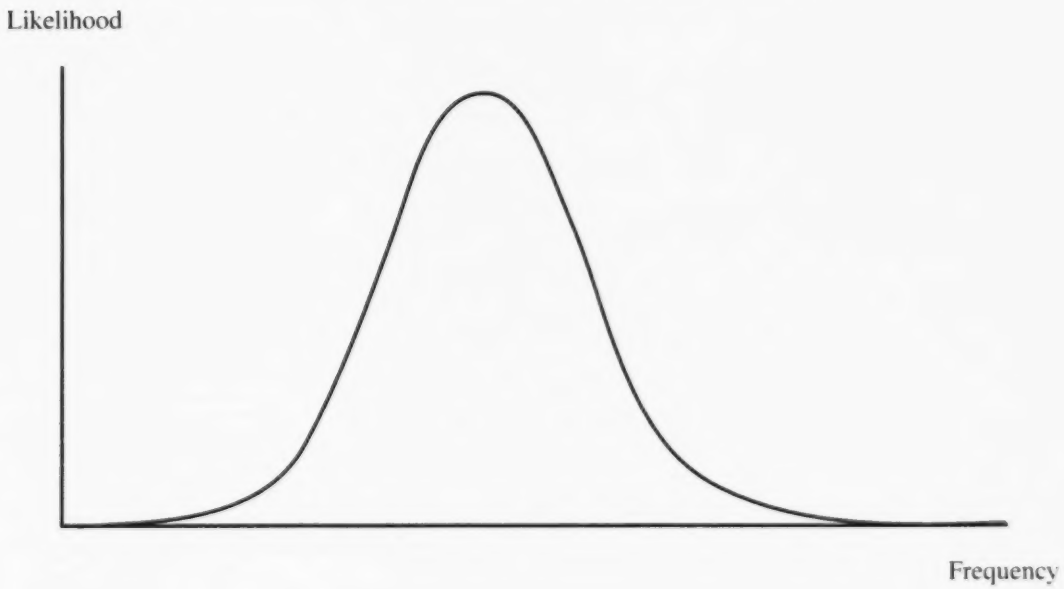


Figure 3: Loss Distribution

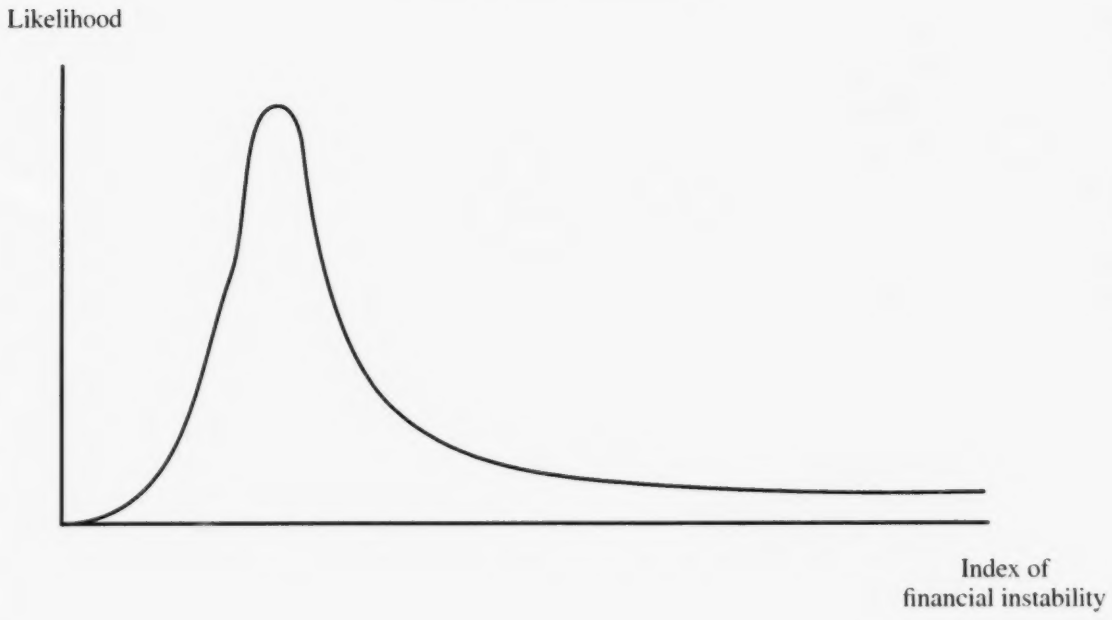


Figure 4: Loss Distribution Associated with CLS

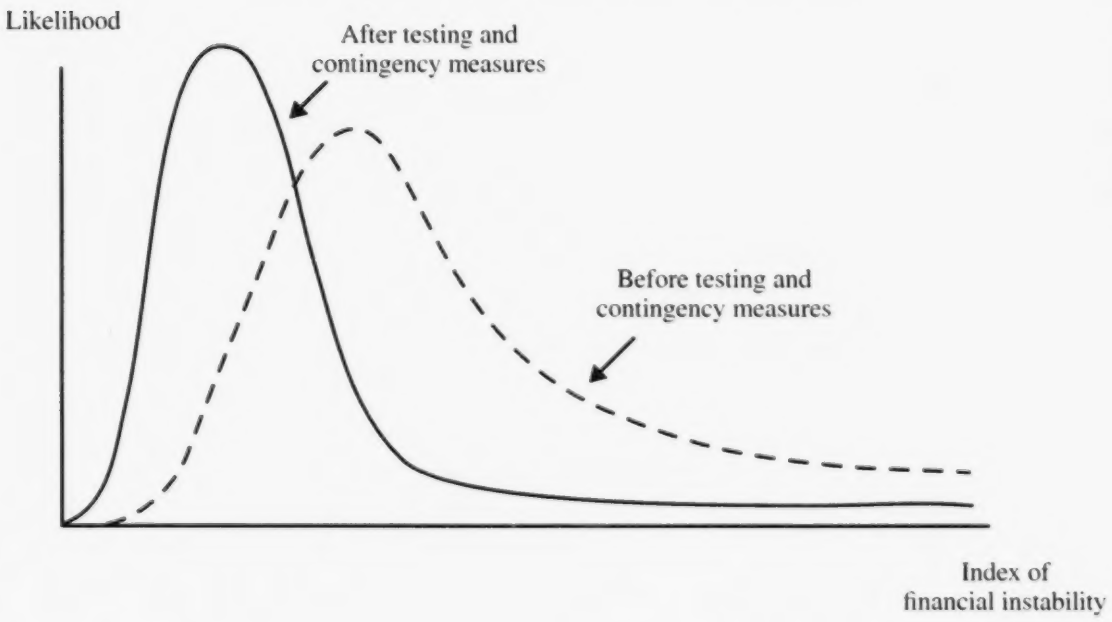


Figure 5: Scorecard Approach

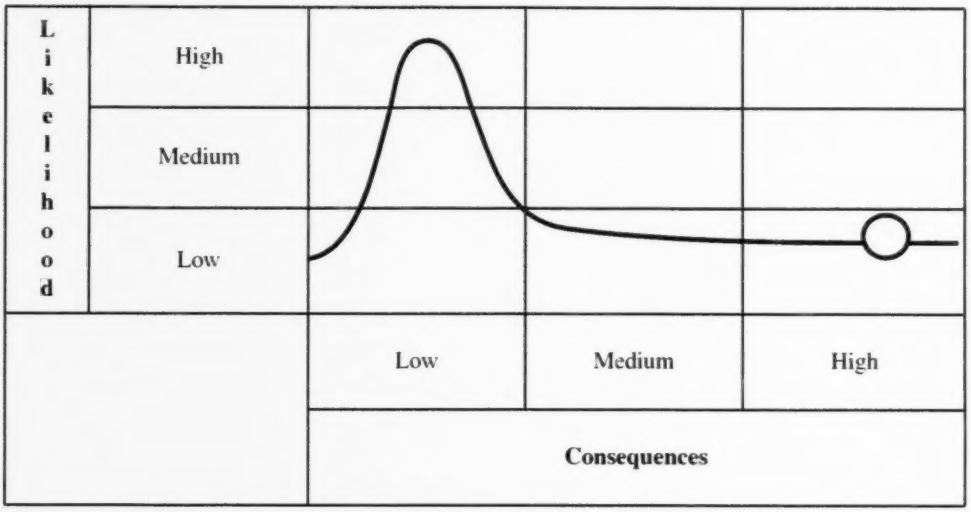
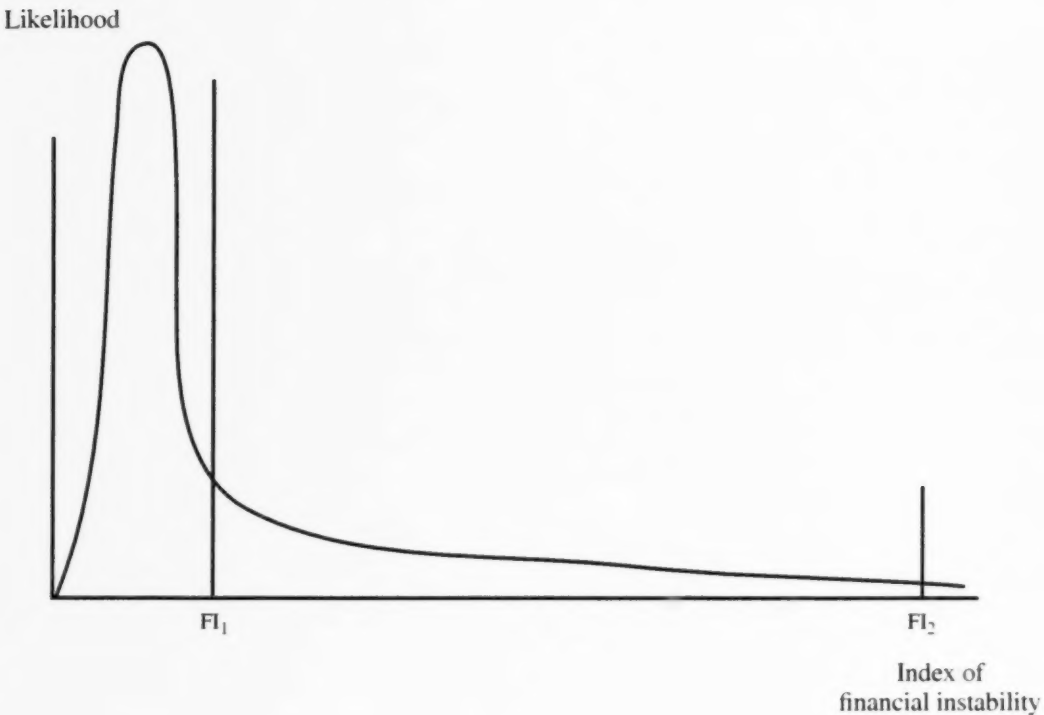


Figure 6: Loss Distribution for PCSS



Appendix A: Recent Regulatory Developments with Respect to Operational Risk in Financial Institutions

In the past five years, the Basel Committee on Banking Supervision of the BIS has focused a considerable amount of attention on operational risk. In 1999, the Committee surveyed a number of large financial institutions. It found that operational risk awareness had increased significantly, although many banks remained at early stages of developing an operational risk-measurement and risk-monitoring framework (BIS 1998c). Further surveys in 2000 suggested that attempts by banks to quantify operational risk were at early stages of development, although many banks had begun (or will begin in the near future) to collect data, track indicators, and investigate quantitative approaches to operational risk measurement (BIS 2001c). Most banks—whether using a purely qualitative approach or developing an approach that adds quantitative elements—lacked an integrated operational risk-management process; that is, strong corporate-governance mechanisms, a consistently applied operational risk definition, data collection, risk assessment and management, and capital allocation. Many banks, however, revealed a high degree of senior management commitment to developing a sound, effective, and integrated operational risk-management framework. These banks anticipate substantial progress in implementing a strong operational risk-management process over the next few years. To guide banks in this process, the Basel Committee published *Sound Practices for Operational Risk Management* in December 2001 (BIS 2001). A revised version was published in July 2002 (BIS 2002a).

In January 2001, the Committee released a draft version of a new Capital Accord. The new Accord has three pillars, each of which has implications for the management of operational risk. Current plans are to begin implementing the new Accord at the end of 2006.

The first pillar of the new Accord proposes several methods, from relatively simple to more advanced, for calculating capital charges related to operational risk. The loss-distribution approach is one of the more advanced approaches that banks may be permitted to use when they can demonstrate that qualitative aspects of operational risk management are robust and that measurement of risk exposures is well-founded.[1]

The second pillar of the new Accord deals with the supervisory review process of the capital adequacy of financial institutions. Part of this review process would be to examine the adequacy of a bank's systems for identifying, analyzing, monitoring, and controlling operational risk.

---

1. Although the loss-distribution approach is relatively new to the operational risk literature, it has been used for more than 30 years in the actuarial sciences.

The third pillar of the new Accord addresses disclosure of operational risk exposure and management (as well as disclosure of other types of risk). Views on the optimal level of disclosure have continued to evolve since the draft of the new Accord was published. A more recent Basel Committee document, *Sound Practices for the Management and Supervision of Operational Risk*, recommends that banks disclose their operational risk-management framework in a way that allows investors and counterparties to determine whether a bank effectively identifies, assesses, monitors, and controls operational risk (BIS 2002b). These disclosure elements, if adopted, would serve as an important additional impetus for financial institutions to establish sound operational risk-management processes.

The Basel Committee recognizes that sound operational risk management requires a sound conceptual framework and a transparent methodology (BIS 2001). The results of risk management should be incorporated into decision-making and into day-to-day activities. There should be ongoing evaluation of risk management relative to objectives, and there should be clear reporting of the results.

Bank of Canada Working Papers
Documents de travail de la Banque du Canada

Working papers are generally published in the language of the author, with an abstract in both official languages. ***Les documents de travail sont publiés généralement dans la langue utilisée par les auteurs; ils sont cependant précédés d'un résumé bilingue.***

2003

2003-1	Banking Crises and Contagion: Empirical Evidence	E. Santor

2002

2002-42	Salaire réel, chocs technologiques et fluctuations économiques	D. Tremblay
2002-41	Estimating Settlement Risk and the Potential for Contagion in Canada's Automated Clearing Settlement System	C.A. Northcott
2002-40	Inflation Changes, Yield Spreads, and Threshold Effects	G. Tkacz
2002-39	An Empirical Analysis of Dynamic Interrelationships Among Inflation, Inflation Uncertainty, Relative Price Dispersion, and Output Growth	F. Vitek
2002-38	Oil-Price Shocks and Retail Energy Prices in Canada	M. Chacra
2002-37	Alternative Public Spending Rules and Output Volatility	J.-P. Lam and W. Scarth
2002-36	Une approche éclectique d'estimation du PIB potentiel américain	M.-A. Gosselin et R. Lalonde
2002-35	The Impact of Common Currencies on Financial Markets: A Literature Review and Evidence from the Euro Area	L. Karlinger
2002-34	How Do Canadian Banks That Deal in Foreign Exchange Hedge Their Exposure to Risk?	C. D'Souza
2002-33	Alternative Trading Systems: Does One Shoe Fit All?	N. Audet, T. Gravelle, and J. Yang
2002-32	Labour Markets, Liquidity, and Monetary Policy Regimes	D. Andolfatto, S. Hendry, and K. Moran
2002-31	Supply Shocks and Real Exchange Rate Dynamics: Canadian Evidence	C. Gauthier and D. Tessier
2002-30	Inflation Expectations and Learning about Monetary Policy	D. Andolfatto, S. Hendry, and K. Moran
2002-29	Exponentials, Polynomials, and Fourier Series: More Yield Curve Modelling at the Bank of Canada	D.J. Bolder and S. Gusba

Copies and a complete list of working papers are available from:
Pour obtenir des exemplaires et une liste complète des documents de travail, prière de s'adresser à :

Publications Distribution, Bank of Canada
234 Wellington Street, Ottawa, Ontario K1A 0G9
E-mail: publications@bankofcanada.ca
Web site: http://www.bankofcanada.ca

Diffusion des publications, Banque du Canada
234, rue Wellington, Ottawa (Ontario) K1A 0G9
Adresse électronique : publications@banqueducanada.ca
Site Web : http://www.banqueducanada.ca